Oregon Department of Justice
FINANCIAL FRAUD/CONSUMER PROTECTION SECTION

SCAM ALERT

Attorney General Ellen Rosenblum Warns Oregon Nonprofits to Watch Out for Phony Donors

The Department of Justice is warning Oregon nonprofit organizations and consumers to be on the lookout for an "overpayment" donation scam that has targeted at least two local charities.

Here's how the scam works: the Oregon nonprofit receives notice from their credit card or online processing company of a large donation, $3,300 for example. Using contact information provided by the supposed donor, the organization sends an acknowledgement email thanking them for their gift. Almost immediately the phony donor replies, stating he or she made a mistake and only intended to donate $300. The donor then asks the charity to issue a $3,000 refund to a card number different from the one used to make the donation. Thankfully, the organizations that complained to DOJ recognized that something was wrong and didn't take the bait.

This is just one variation of refund fraud perpetrated by scam artists who are typically located overseas. In this particular scheme the scammer will make a charitable donation with a stolen credit card and use the nonprofit as a conduit to launder funds into his or her own coffers. The crime is particularly harmful because it victimizes both the consumer whose credit card was stolen, as well as nonprofit organizations that rely on donor contributions for their programs. The same pattern of activity can also affect businesses that issue refunds from their own bank account before learning the original transaction was invalid. Although fraudulent credit card charges can be disputed, victims who issue refunds have very little recourse because the phony donor is likely outside the U.S.

So how can one tell the difference between a legitimate donation and a con? Attorney General Rosenblum offers the following suggestions:

1. **Contact DOJ**. The Department of Justice's Charitable Activities Section administers state laws governing charitable and other nonprofit organizations in Oregon. If you or someone you know has experienced a scam or fraud involving

a charity, contact the Charitable Activities Section at charitable.activities@state.or.us or 971-673-1880. The section's staff may be able to provide guidance and help prevent other organizations from falling prey to these schemes.

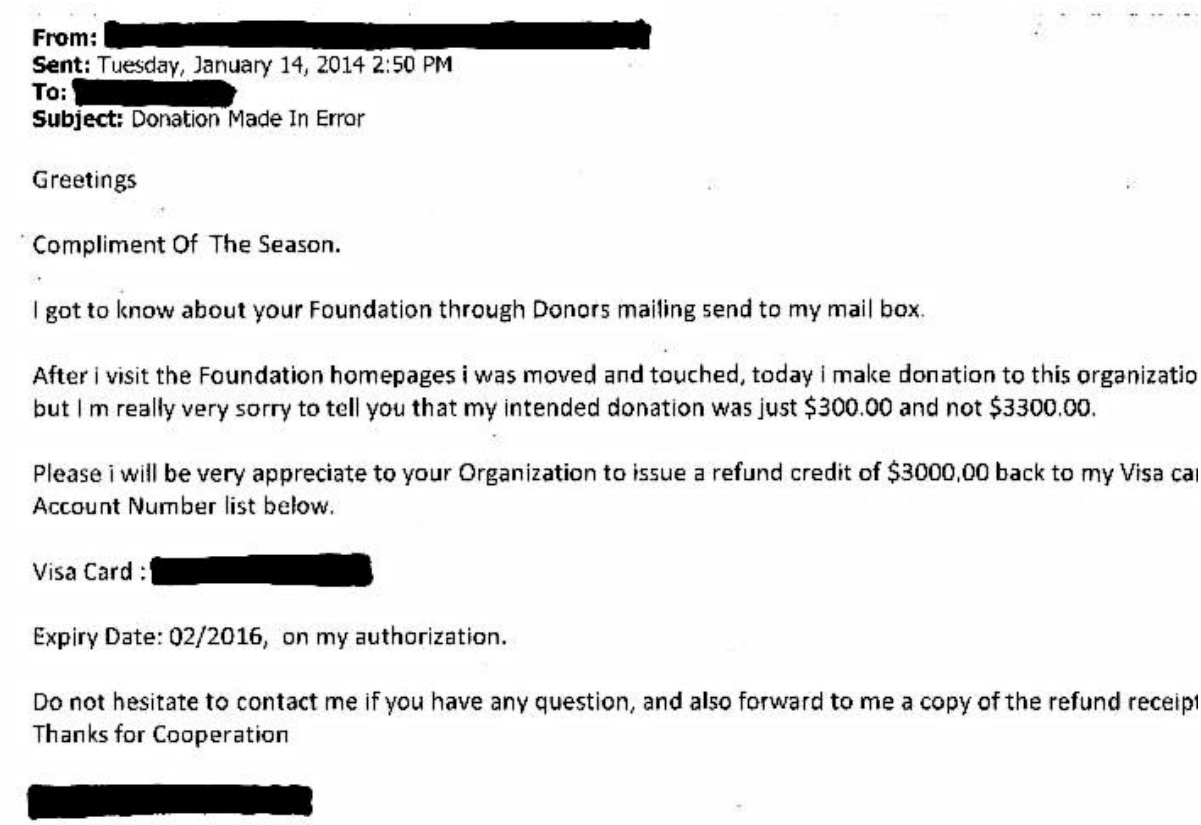
2. **You wire it, you lose it**. Never send money via wire transfer, money order or a pre-paid debit card, like Green Dot Money Pack. These methods of payment provide little or no recourse for scam victims and present obstacles for law enforcement in identifying the thief.

3. **Exercise vigilance**. Guard your nonprofit and personal account information carefully and check transaction reports on a regular basis. If you notice suspicious activity, contact your merchant processing company or financial institution to report the suspected fraud. Consumers should beware of any small donations or other transactions that show up on their credit card or bank statements; scammers will often use "microcharges" to check whether a stolen credit card number is valid. Consumers should contest any suspicious charge with their credit card issuer right away to avoid a bigger problem in the future.

4. **Spread the word**. Notify employees and board members about charitable donation scams and educate them on preventing your organization from fraud.

5. **Know your donor**. If you receive a contribution from an uncommon source or unusual donor (outside the geographic location of most donors), seek out additional information before issuing a refund. If possible, find out whether the person's identity is in a pre-existing donor database; you could also try searching their name, contact information or e-mail account on the internet.
Ask the donor about the reason for their donation. Be extremely skeptical if he or she is unfamiliar with your basic programs or services.

6. **Recognize warning signs**. Common characteristics of donation or "overpayment" scams include abnormally large contributions and requests for refunds in a different form of exchange than the original payment or donation was made. Watch out for refund requests that include poor grammar, spelling and sentence structure; broken English is a common trait of communications originating overseas. The following email is a real-life example:



From: [redacted]
Sent: Tuesday, January 14, 2014 2:50 PM
To: [redacted]
Subject: Donation Made In Error

Greetings

Compliment Of The Season.

I got to know about your Foundation through Donors mailing send to my mail box.

After i visit the Foundation homepages i was moved and touched, today i make donation to this organizatio
but I m really very sorry to tell you that my intended donation was just $300.00 and not $3300.00.

Please i will be very appreciate to your Organization to issue a refund credit of $3000.00 back to my Visa ca
Account Number list below.

Visa Card : [redacted]

Expiry Date: 02/2016, on my authorization.

Do not hesitate to contact me if you have any question, and also forward to me a copy of the refund receipt
Thanks for Cooperation

[redacted]

7. **Limit your form of refund**. Never issue a check or hand out cash for any credit card transaction. Limit card refunds to the card used in the original transaction. This will prevent the scammer from getting their hands on money in the form they can use.

8. **Report fraud**. If your organization is the target of a charitable donation scam, file a report with the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center. You can file a complaint online at http://1.usa.gov/1kEEOfF.